

оружия, отнесения их к категории боеприпасов и определения пригодности их для стрельбы.

УДК 343.98

В. М. Логвин

*профессор кафедры криминалистики
Академии МВД Республики Беларусь,
кандидат юридических наук, доцент*

О НЕКОТОРЫХ ПРОБЛЕМНЫХ ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Несколько последних десятилетий радикально изменили облик цивилизованного мира. Важнейшим фактором такого изменения оказался научный прогресс. С уверенностью можно констатировать, что произошел переход от индустриального общества к обществу информационному. На это указывают изменения, вызванные информационными технологиями: структурные изменения в экономике, особенно в сфере распределения рабочей силы; возросшее осознание важности информации и информационных технологий; растущее осознание необходимости компьютерной грамотности; широкое распространение компьютеров и информационной технологии; развитие компьютеризации и информатизации общества и образования; поддержка правительством развития компьютерной микроэлектронной технологии и телекоммуникаций; широкое распространение компьютерных вирусов и вредоносных программ по всему миру.

Во время научно-технического прогресса появилась возможность для быстрого и эффективного развития как государства в целом, так и отдельно взятого гражданина за счет внедрения компьютеризации и информатизации общества. В повседневный обиход современного человека вошли персональные компьютеры, планшеты, мобильные телефоны, другая цифровая техника, которая в значительной степени облегчает решение различных задач в процессе жизнедеятельности человека. Разнообразие такой техники имеет стойкую тенденцию к увеличению и расширению. Представить себе жизнь человека без названных достижений научно-технического прогресса достаточно сложно.

Вместе с тем различные программно-технические устройства используются не только во благо человека, но и способствуют изменению характера многих общественных отношений, возникновению новых видов преступлений, о которых еще совсем недавно никто не мог подумать. Об этом свидетельствует рост количества преступлений, совершаемых с использованием компьютерной техники и компьютерной ин-

формации. Причем речь идет не только о преступлениях в сфере информационной безопасности, но и о традиционных (незаконный оборот наркотиков, фальшивомонетничество, мошенничество и др.).

Если в конце XX века правоохранительным органам приходилось сталкиваться с единичными случаями совершения таких преступлений, к совершению которых имели отношение малоподготовленные молодые люди, то в настоящее время компьютерная преступность превратилась в одну из сфер приложения усилий криминала, характеризующихся организованным характером действий, специализацией и разделением функций преступников и их высоким профессионализмом. В этой связи выявление (раскрытие), расследование и предупреждение таких преступлений является весьма затруднительным делом. Серьезным препятствием для борьбы с компьютерной преступностью является высокая латентность преступлений в сфере информационной безопасности. По данным криминологов на одно учтенное деяние 4–5 реально совершаемых преступлений остаются латентными, а следовательно, и безнаказанными.

Что может противопоставить общество, государство этому направлению криминальной деятельности? Не претендуя на исчерпывающий перечень мер в плане противодействия преступлениям в сфере информационной безопасности, хотелось бы обратить внимание на следующие обстоятельства.

1. Киберпреступность в последнее время становится, с этим уже сложно спорить, одной из доминирующих форм преступности не только в Республике Беларусь, СНГ, но и странах всего мира. Феномен компьютерной преступности требует детальнейшего изучения представителями различных направлений юридической науки и прежде всего криминологами. В то же время анализ юридической литературы позволяет утверждать, что этой проблеме уделяется не достаточно внимания. Подтверждение тому – отсутствие фундаментальных научных исследований, посвященных изучению проблемы компьютерной преступности как явления, охватывающих собой весь спектр преступлений, относящихся к этой сфере. В основном работы белорусских ученых посвящены вопросам совершенствования уголовной ответственности за совершение преступлений в сфере информационной безопасности, имеются отдельные публикации, где исследуются вопросы криминологической характеристики преступлений, относящихся к данной сфере. На наш взгляд, данное обстоятельство свидетельствует о том, что правоохранительная система пока находится в поиске не только методов борьбы с этой проблемой, но и в процессе выработки единой политики по этому вопросу, в том числе и понятийного аппарата (отсутствие четкого анализа проявлений преступности, прогноза на будущее, стратегии борьбы с этим явлением, ненадлежащее законодательное обеспечение противодействия

данному явлению, слабая готовность правоохранительных органов к борьбе с преступностью в области информационной безопасности и др.).

2. Важнейшее значение в противодействии киберпреступности имеет деятельность правоохранительных органов Республики Беларусь по выявлению (раскрытию), расследованию и предупреждению криминальных деяний, относящихся к преступлениям в сфере информационной безопасности. Решение этой задачи в основном возложено на сотрудников управления по раскрытию преступлений в сфере высоких технологий (управление «К») МВД Республики Беларусь и следователей Следственного комитета Республики Беларусь. Комплектование вакантных должностей в оперативно-розыскном подразделении МВД осуществляется, как правило, за счет лиц, имеющих соответствующее образование в области IT-технологий. В дальнейшем сотрудники управления «К» имеют возможность получения юридического образования в вузах Республики Беларусь.

Должности следователей подразделений Следственного комитета Республики Беларусь комплектуются лицами, имеющими высшее юридическое образование. Так называемые технари в среде следователей – явление исключительное. Как правило, это лица, овладевшие самостоятельно знаниями в области IT-технологий и виртуозно владеющие компьютером. Мы не ставим перед собой цель проведения анализа качественного состава названных подразделений, но в целом следует отметить, что на текущий момент сотрудники и одной и другой правоохранительных структур успешно справляются со стоящими перед ними задачами. Тем не менее необходимо обратить внимание на несколько иное обстоятельство, которое может существенно повысить эффективность противодействия преступности в сфере информационной безопасности. На текущий момент выявлением (раскрытием), расследованием, предупреждением таких преступлений в основном занимаются штучные специалисты, проходящие службу в подразделениях указанных правоохранительных органов. С учетом общемировых тенденций относительно роста количества регистрируемых преступлений в сфере информационной безопасности, использования цифровых технологий при совершении преступлений этого явно недостаточно. Очевидно, умениями и навыками по выявлению (раскрытию), расследованию и предупреждению подобных преступлений должны обладать сотрудники и иных подразделений МВД, Следственного комитета Республики Беларусь, деятельность которых напрямую не связана с противодействием киберпреступности. Такой подход позволит в значительной степени повысить общий профессиональный уровень сотрудников правоохранительных структур, будет способствовать повышению эффективности борьбы с преступлениями в сфере высоких технологий и борьбе с преступностью

в целом. Эта мера будет способствовать готовности правоохранительных органов противостоять преступности в целом.

3. Правоохранительная практика показывает, что успешную борьбу с преступностью могут осуществлять лишь всесторонне профессионально подготовленные сотрудники при условии безупречной организации и взаимодействия в процессе выполнения своих служебных обязанностей. Для успешного выявления (раскрытия), расследования и предупреждения преступлений большое значение имеет криминалистика и разрабатываемые ею соответствующие технические средства, тактические приемы и методы расследования преступлений. В этой связи исключительно актуальной является проблема профессиональной, в том числе криминалистической подготовки сотрудников правоохранительных органов, привития будущим и действующим сотрудникам специальных практических навыков, связанных с криминалистическим обеспечением выявления (раскрытия), расследования и предупреждения преступлений в сфере компьютерных технологий.

Следует отметить, что решение этой простой, на первый взгляд понятной задачи осложняется рядом негативных обстоятельств. За последние несколько десятков лет произошли существенные изменения в подходах к обучению не только криминалистике, но и многим другим специальным дисциплинам, которые ранее определяли качественный уровень подготовки выпускника вуза с квалификацией «юрист». Криминалистика как учебная дисциплина превратилась во второсортный учебный курс. На протяжении всего этого времени неоднократно предпринимались попытки «урезать» учебный курс, которые были достаточно успешными. Ситуация существенно ухудшилась в последние 10 лет, в течение которых криминалистика в результате «совершенствования» образовательных стандартов по специальности «Правоведение» не нашла своего места в перечне специальных дисциплин по данной специальности. В учебных планах вузов в разделе цикла специальных дисциплин в зависимости от специализации она была сохранена лишь благодаря доброй воле членов научного совета того или иного вуза.

Анализ содержания учебно-методической документации, учебников, пособий по учебной дисциплине «Криминалистика» для различных специальностей обучения свидетельствует о том, что содержание учебной дисциплины «застыло» на рубеже 80-х годов прошлого века. Как правило, вся программная документация, а соответственно и вся учебная литература, строятся на традиционных знаниях и представлениях о криминалистике. Например, применительно к предмету нашего исследования, как правило, в учебных программах по специальности «Правоведение» упоминается лишь тема «Методика расследования преступлений в сфере информационной безопасности», где рассматриваются, как правило, лишь рекомендации общего характера относительно рассле-

дования достаточно большой группы преступлений. Вместе с тем учебно-программная документация не содержит следующих сведений: о современной системе следов в криминалистике; о понятии и значении виртуальных следов; о возможностях обнаружения, фиксации, изъятия, обеспечения сохранности виртуальных следов в ходе проведения отдельных следственных действий; возможностях экспертного исследования таких следов либо их носителей и использования результатов исследований в целях доказывания отдельных обстоятельств совершенного преступления. Представляется, что без глубокого изучения перечисленных вопросов изучение основ методики расследования преступлений в сфере информационной безопасности является делом весьма проблематичным. Причинами такого положения дел являются: посредственные знания преподавательского состава в области информационных технологий; игнорирование одного из принципов обучения «от общего к частному, от главного к второстепенному, от традиционного к новому»; отсутствие у заказчика четких представлений о том, что должен знать, уметь и чем должен владеть выпускник вуза; отсутствие реального взаимодействия между учебным заведением и заказчиком, которое как минимум предполагает: предоставление заказчиком учебному заведению статистической, аналитической и иной необходимой для образовательного процесса информации, выборочный доступ преподавательского состава к материалам проверок, уголовным делам находящимся в производстве, приостановленных и прекращенных производством по различным основаниям, возможность использования их в учебном процессе и др. Устранение перечисленных и иных причин может в значительной степени повысить эффективность образовательного процесса, уровень овладения выпускниками вузов и других категорий обучаемых теоретическими знаниями, сформировать должный уровень умений и навыков, который позволит эффективно противодействовать киберпреступности и преступности в целом.

В заключение следует отметить, что проблема противодействия киберпреступности носит комплексный характер. Ее решение связано с проведением научных исследований прежде всего в области криминологии, уголовного права, уголовного процесса, криминалистики, оперативно-розыскной деятельности и других наук. Выработка четких предложений по противодействию киберпреступности будут способствовать обеспечению цели и задач концепции национальной безопасности Республики Беларусь.